Unicorns and Air Gaps – Do They Really Exist?

Living with Reality in Critical Infrastructures

Eric Byres, P.Eng.
CTO and VP Engineering, Tofino Security
Part of Belden Inc.

HIRSCHMANN
A BELDEN BRAND

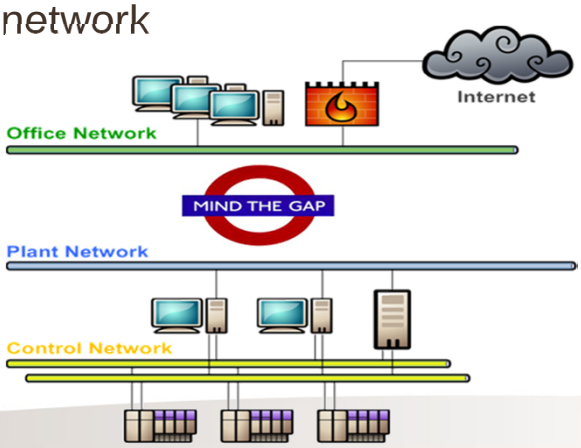
TOFINO™

The Amazing Air Gap…

TOFINO™

What is an Air Gap?

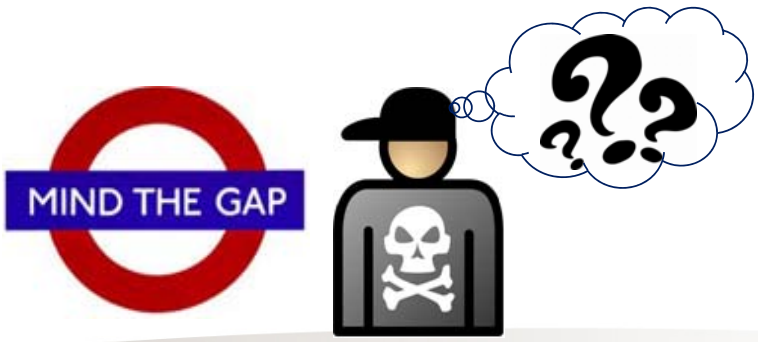
- A physical gap between the control network and the business network



TOFINO™

Why is An Air Gap an Attractive Idea?

1. Digital information cannot cross a physical gap
2. Bad things will never get into control systems



TOFINO™

Who Believes in Air Gaps?

- Vendor PR managers…

  "It is important to ensure your automation network is protected from unauthorized access using the strategies suggested in this document or isolate the automation network from all other networks using an air gap."

  (Source: SIEMENS-SSA-625789: Security Vulnerabilities in Siemens SIMATIC S7-1200 CPU, June 2011)

TOFINO™

Who Believes in Air Gaps?

- Security bloggers:

  "I've written about SCADA issues in the past, but one issue that I've consistently tried to emphasize is that critical control systems should never, ever interact nor interconnect with Internet systems in any way, shape, or form. There's a good reason for this, and it's always been referred to as the "Air Gap" Principle.."

  (Source: Paul Ferguson, Internet Security Intelligence Advanced Threats Research, Trend Micro, Apr 8, 2012)

TOFINO™

Who Does NOT Believe in Air Gaps?

- Vendor engineering managers:

  "*Forget the myth of the air gap – the control system that is completely isolated is history.*"

  (Source: Stefan Woronka, Siemens Director of Industrial Security Services, Siemens Summit , July 2011)

TOFINO™

Who Does NOT Believe in Air Gaps?

- US Government ICS-CERT Reports:

  "*ICS-CERT recommends placing all control systems assets behind firewalls, separated from the business network*."

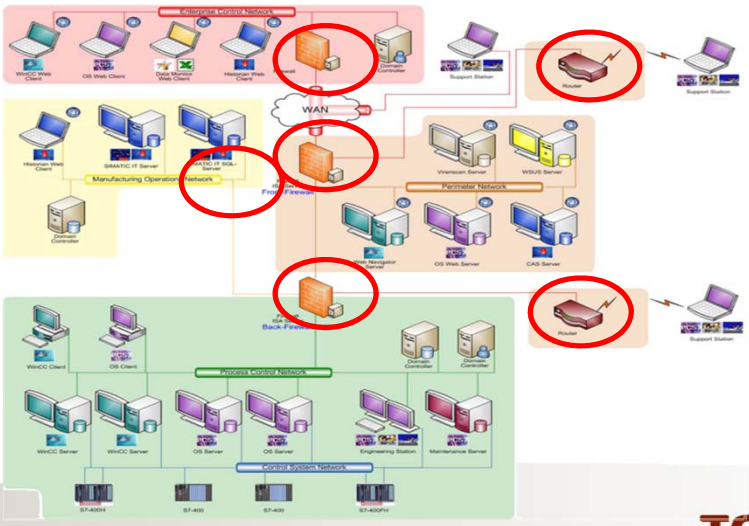
  (Source: Multiple ICS-CERT Advisories)

TOFINO™

Searching for Air Gaps

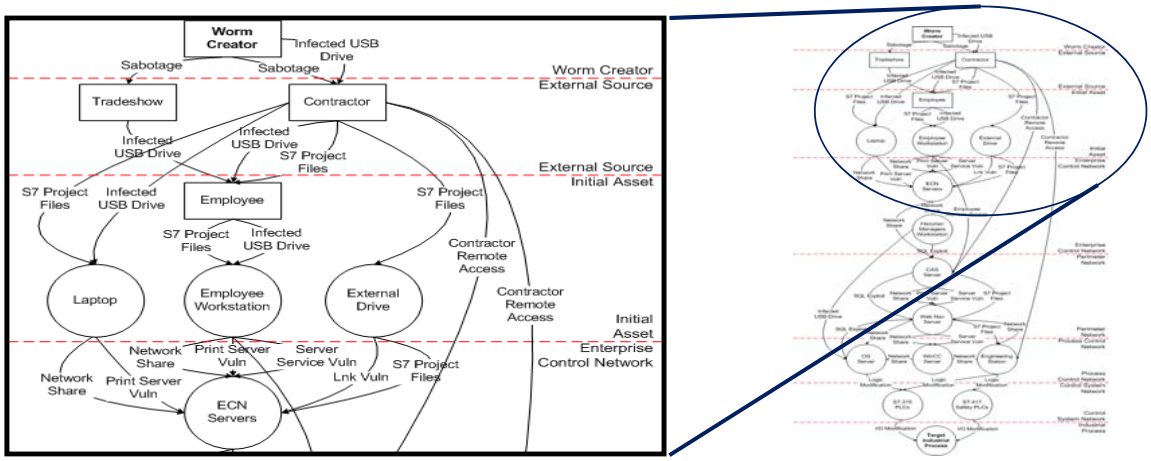
TOFINO™

Looking in Vendor Manuals



TOFINO™

Let's Look at Stuxnet…



TOFINO™

Let's Ask the Dept of Homeland Security

"In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network.

On average, we see 11 direct connections between those networks."

Source: Sean McGurk, The Subcommittee on National Security, Homeland Defense, and Foreign Operations May 25, 2011 hearing.

TOFINO™

We Found One!

TOFINO™

The Challenge of Air Gaps

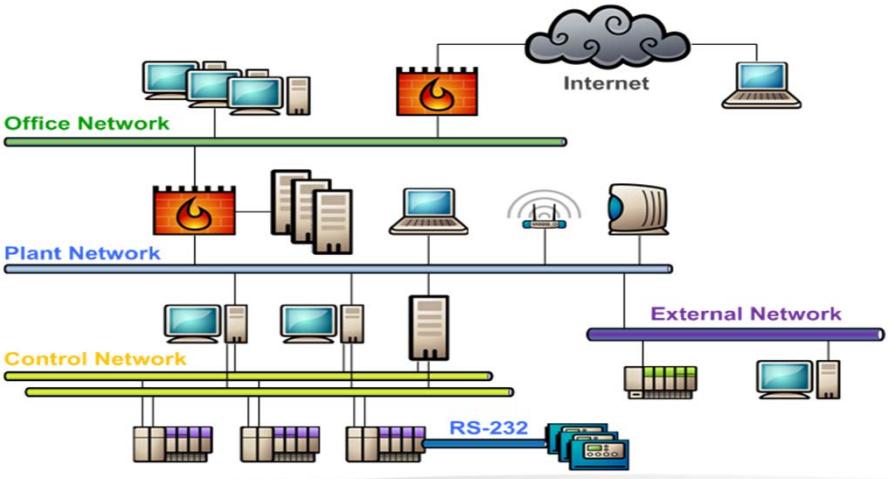
TOFINO™

The Control Systems' Hunger for Data

- New logic from the engineering consultant that addresses a design flaw causing downtime
- Adobe sends you an update for a critical vulnerability in the PDF Reader
- The lab sends a new recipe that will improve quality
- Patches for computer operating systems
- Anti-virus signatures and white lists
- Remote support by system experts

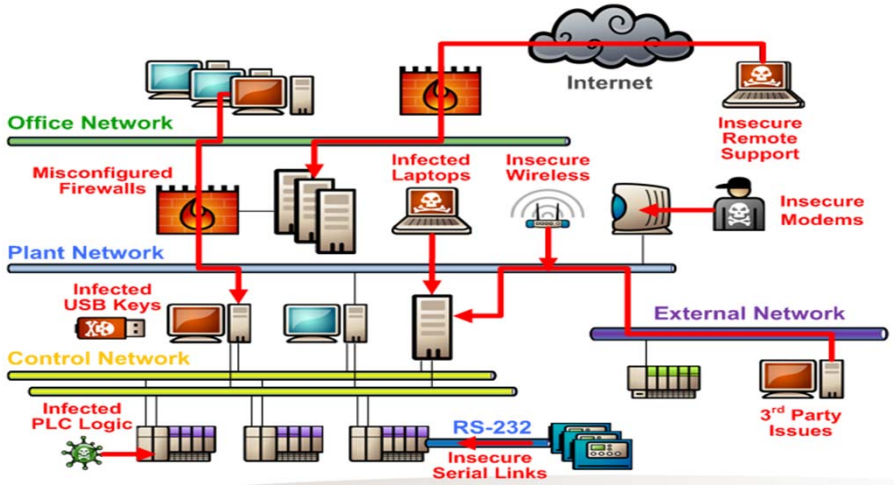
TOFINO™

Pathways into the Plant Floor



TOFINO™

Pathways into the Plant Floor



TOFINO™

It is not a Technology Issue

- The air gap leads to a false sense of security:

  "*None of the vulnerabilities [uncovered at the NESCOR summit] pose as great a risk as the belief that your system is isolated*."

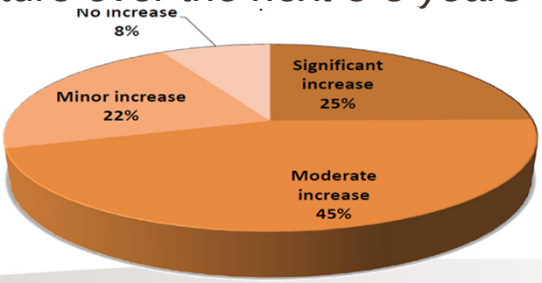
  Chris Blask, CEO, ICS Cybersecurity Inc.

- Air gaps divert data flow to “sneakernet” channels
- Companies lack controls to manage information over “sneakernet” channels

TOFINO™

It is Going to Get Worse…

- *"71% of control engineers expect to see either significant or moderate increases in connectivity between industrial endpoints and corporate IT infrastructure over the next 3-5 years "*



Source: Managing Automation Systems: Critical Infrastructure Operators' Challenges & Opportunities, Industrial defender, 2011

TOFINO™

What Does It All Mean?

- Assuming an air-gap between ICS and corporate networks is unrealistic
- Modern ICS or SCADA systems are highly complex
- Multiple potential pathways exist from the outside world to the process controllers
- Focusing security efforts on a few obvious pathways (such as USB storage drives or the Enterprise/ICS firewall) is a flawed defense

TOFINO™

Real World Security for Control Systems

TOFINO™

Security Solutions Must Fit with Human Nature

- Is the problem with the air gap a people problem?
- No – any technology that requires the user to act in ways that are counter to human nature is flawed
- Expecting engineers to act in ways that are counter to their job goals is asking for trouble

TOFINO™

Practical Solutions for ICS/SCADA Security

- Manage ALL data flows into ICS
- Manage ALL data flows out of ICS
- Subdivide ICS systems so that issues don't spread
- Detect unusual behaviors in ICS systems
- Progressively reduce the probability of attacker success the deeper they go into the system

TOFINO™

ANSI/ISA-99: Dividing Up The Control System

- A core concept in the ANSI/ISA-99 (now ISA/IEC 62443.02.01) security standard is "Zones and Conduits"
- Defines segmentation inside the control system
- ICS networks divided into layers or zones based on control function
- Multiple separated zones manage that "***defense in depth***" strategy

TOFINO™

ANSI/ISA-99: Connecting the Zones

- Connections between the zones are called conduits, and these must have security controls to:
  - Control access to zones
  - Resist Denial of Service (DoS) attacks or the transfer of malware
  - Shield other network systems
  - Protect the integrity and confidentiality of network traffic
- It is important to understand and manage all your conduits between zones, not just the obvious ones

TOFINO™

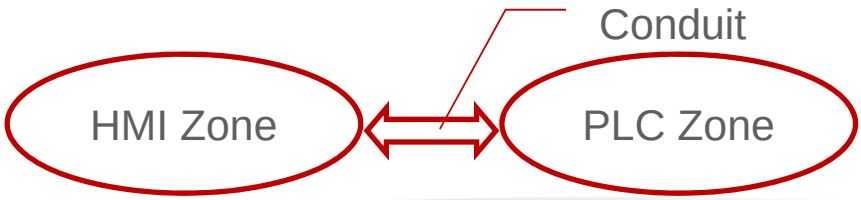
Security Zone Definition

- "Security zone: grouping of logical or physical assets that share common security requirements" [ANSI/ISA-99.02.01–2007- 3.2.116]
  - A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements

TOFINO™

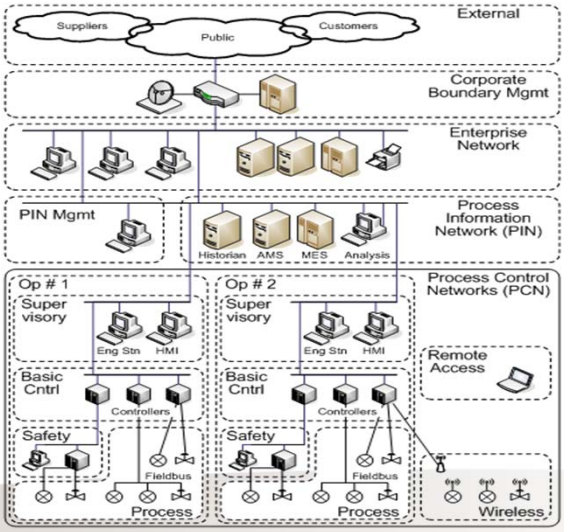
Conduits

- A conduit is a path for the flow of data between two zones
  - can provide the security functions that allow different zones to communicate securely
  - Any communications between zones must have a conduit.



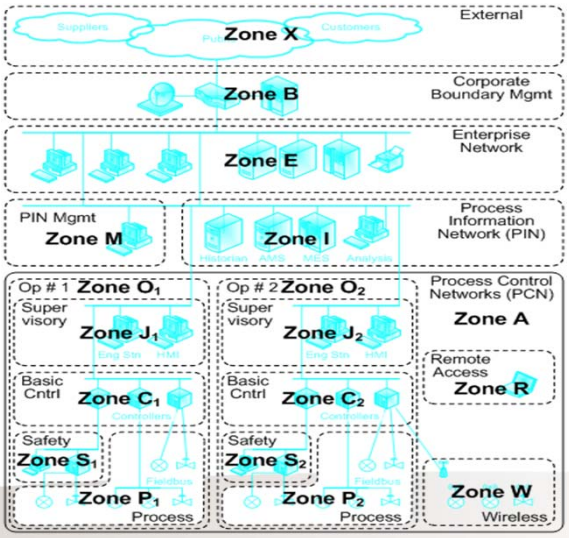
TOFINO™

Using Zones: An Example Oil Refinery



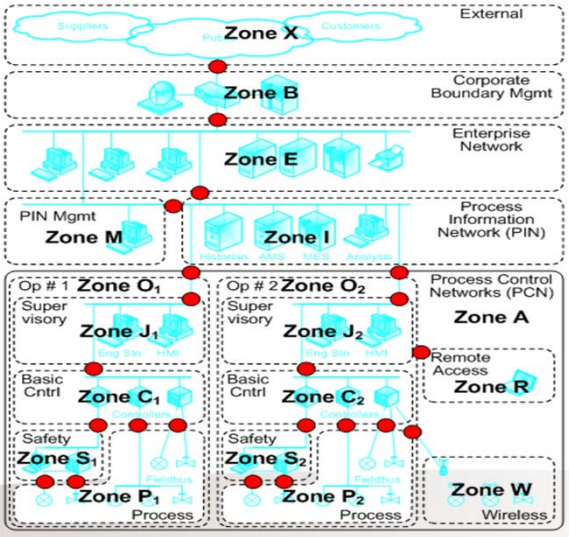
TOFINO™

Specifying the Zones



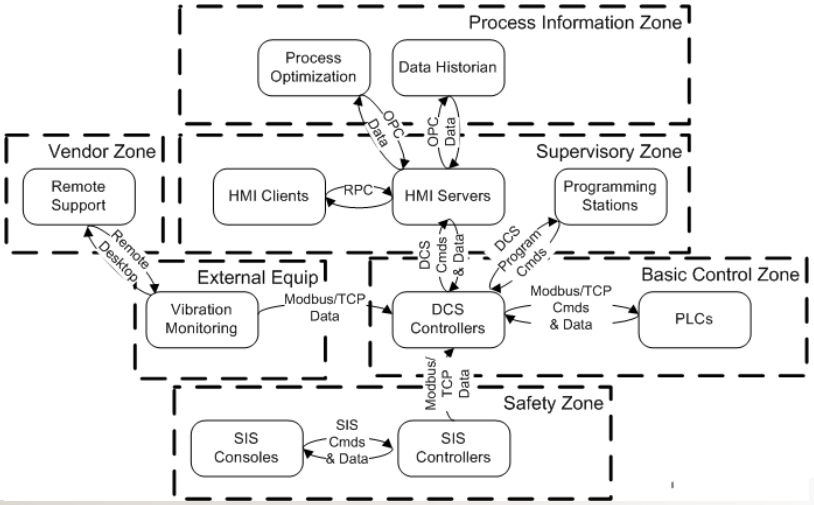
TOFINO™

Defining the Conduits



TOFINO™

Defining the Data Flow Between Zones

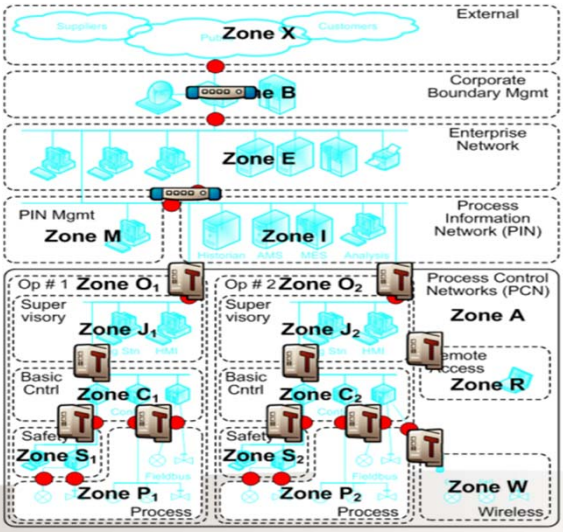


TOFINO™

Protecting with Process and Technology

Corporate Firewall

Tofino Firewall



TOFINO™

Look At All Possible Pathways

- Don’t focus on a single pathway such as the network
- Consider all possible infection pathways:
  - Removable Media (CDs, DVDs, USB Drives)
  - File Transfer (Database, PDFs, PLC Project Files)
  - Portable Equipment (Laptops, Storage Units, Config Tools)
  - Internal Network Connections (Business, Lab, QA, Support)
  - External Connections (Support, Contractor, Customer)
  - Wireless (802.11, 802.15, Licensed-band, Cellular,etc)
  - Other Interfaces (Serial, Data Highways)

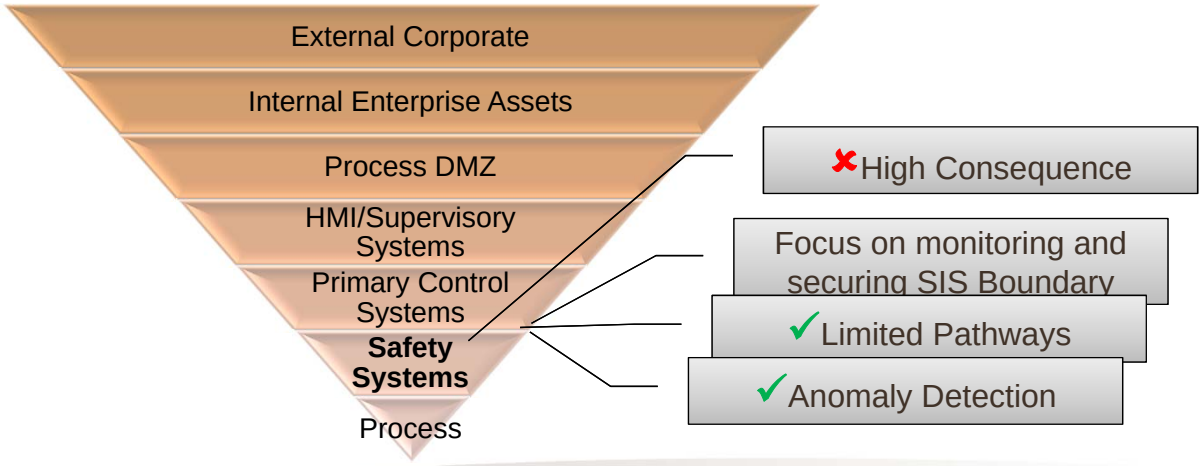
TOFINO™

Look At All Possible Pathways

- Have strategies for discovering/mitigating ALL pathways

TOFINO™

Start with Last-line-of-Defense Critical Systems



TOFINO™

SCADA/ICS-Appropriate Technologies

- Deploy ICS-appropriate security technologies to raise an alarm when equipment is compromised or at risk of compromise
- Look beyond traditional network layer firewalls, towards firewalls that are capable of deep packet inspection of key SCADA and ICS protocols

TOFINO™

Some Closing Thoughts…

- Air gaps are a dangerous illusion
- ICS/SCADA systems need data to function
- Improved defense-in-depth strategies for industrial control systems are the only realistic solution
- Start by securing last-line-of-defense critical systems, particularly safety integrated systems (SIS)

TOFINO™

TOFINO™

tofinosecurity.com

HIRSCHMANN
A BELDEN BRAND